

(19) 日本国特許庁(JP)

(12) **公開特許公報(A)**

(11) 特許出願公開番号

特開2004-145605

(P2004-145805A)

(43) 公開日 平成16年5月20日(2004.5.20)

(51) Int.Cl.⁷

G06F 12/14

G06F 1/00

G06K 19/073

F1

G06F 12/14

G O 6 F 9/06

G O 6 K 19/00

3 1 0 H

660 L

P

テーマコード (参考)

5 B O 1 7

5 B 0 3 5

5 B 0 7 6

審査請求 未請求 請求項の数 9 O L (全 17 頁)

(21) 出題番号

特願2002-309276 (P2002-309276)

(22) 出題日

平成14年10月24日 (2002.10.24)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(74) 代理人 100077931

弁理士 前田 弘

(74) 代理人 100094134

弁理士 小山 廣毅

(74) 代理人 100110939

弁理士 竹内 宏

(74) 代理人 100110940

弁理士 嶋田 高久

(74) 代理人 100113262

弁理士 竹内 祐二

(74) 代理人 100115059

弁理士 今江 克実

最終頁に続く

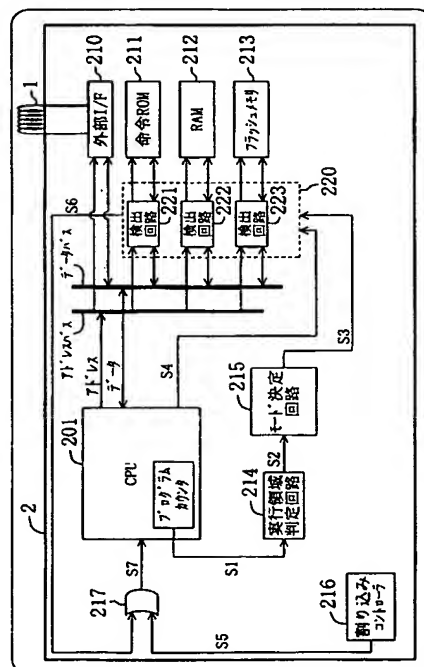
(54) 【発明の名称】 プロセッサ

(57) 【要約】

【課題】 命令ROMとデータメモリと拡張メモリと外部I/Fをもつプロセッサにおいて、外部から拡張メモリにプログラムが追加された場合において、追加されたプログラムによる命令ROMに対する不正読み出しやデータメモリに対する不正読み書きを防止する機構を提供する。

【解決手段】CPUが処理を行う命令のプログラムカウンタの属する領域ごとに動作モードを設け、その動作モードごとに各領域へのアクセス制限を設ける。不正アクセスを検出する不正アクセス検出回路221～223によって、不正なアクセスを検出した場合には割り込みを発生させて、処理を中止させることによって、追加されたプログラムによる不正アクセスを防ぐ。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

外部とのデータのやりとりを行う外部 I / F と、
プログラムを格納する命令 R O M と、
データを格納するデータメモリと、
前記外部 I / F を経由して追加されたプログラムを格納する拡張メモリと、
前記命令 R O M および前記拡張メモリに格納されたプログラムを実行する C P U と、
前記 C P U が実行している命令のプログラムカウンタ値に基づいて実行領域を判定する実行領域判定回路と、
前記実行領域判定回路による判定結果に従って動作モードを決定するモード決定回路と、
前記モード決定回路によって決定された動作モードとアクセスアドレスとによって許可されないアクセスが発生した場合に割り込み要求を出力する不正アクセス検出回路とを備える
ことを特徴とするプロセッサ。

【請求項 2】

請求項 1 において、
前記モード決定回路によって決定される動作モードには、特権モード、A P I モード、ユーザモードが含まれ、
論理アドレス空間は、特権領域、A P I 領域、ユーザ領域の 3 つに区分され、
前記命令 R O M には前記特権領域および前記 A P I 領域、前記データメモリには前記特権領域、前記 A P I 領域および前記ユーザ領域、前記拡張メモリには前記ユーザ領域が割り当てられ、
前記モード決定回路は動作モードを、前記特権領域上のプログラム実行時には特権モード、前記 A P I 領域上のプログラム実行時には A P I モード、前記ユーザ領域上のプログラム実行時にはユーザモードとする
ことを特徴とするプロセッサ。

【請求項 3】

請求項 2 において、
前記不正アクセス検出回路は、
前記モード決定回路によって決定された動作モードが特権モードのとき、前記特権領域、
前記 A P I 領域および前記ユーザ領域へのデータアクセスおよび命令アクセスを許可し、
前記モード決定回路によって決定された動作モードが A P I モードのとき、前記特権領域への命令アクセスと、前記 A P I 領域および前記ユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスを禁止し、
前記モード決定回路によって決定された動作モードがユーザモードのとき、前記 A P I 領域への命令アクセスと、前記ユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスおよび命令アクセスと、前記 A P I 領域へのデータアクセスとを禁止する
ことを特徴とするプロセッサ。

【請求項 4】

外部とのデータのやりとりを行う外部 I / F と、
プログラムを格納する命令 R O M と、
データを格納するデータメモリと、
前記外部 I / F を経由して追加されたプログラムを格納する拡張メモリと、
前記命令 R O M および前記拡張メモリに格納されたプログラムを実行する C P U と、
前記 C P U が実行している命令のプログラムカウンタ値に基づいて実行領域を判定する実行領域判定回路と、
特権フラグと、
前記特権フラグの値を判定する特権フラグ判定回路と、
前記実行領域判定回路による判定結果と前記特権フラグ判定回路による判定結果とに従っ

て動作モードを決定するモード決定回路と、

前記モード決定回路によって決定された動作モードとアクセスアドレスとによって許可されないアクセスが発生した場合に割り込み要求を出力する不正アクセス検出回路とを備える

ことを特徴とするプロセッサ。

【請求項 5】

請求項 4 において、

前記モード決定回路によって決定される動作モードには、特権モード、A P I モード、ユーザモードが含まれ、

論理アドレス空間は、特権領域、A P I 領域、ユーザ領域に区分され、

前記命令 R O M には前記特権領域および前記 A P I 領域、前記データメモリには前記特権領域、前記 A P I 領域および前記ユーザ領域、前記拡張メモリには前記ユーザ領域、前記特権フラグには前記 A P I 領域が割り当てられ、

前記モード決定回路は動作モードを、前記特権領域または前記 A P I 領域上のプログラム実行時でありかつ前記特権フラグが O N のときには特権モード、前記 A P I 領域上のプログラム実行時でありかつ前記特権フラグ O F F のときには A P I モード、前記ユーザ領域上のプログラム実行時にはユーザモードとする

ことを特徴とするプロセッサ。

【請求項 6】

請求項 5 において、

前記不正アクセス検出回路は、

前記モード決定回路によって決定された動作モードが特権モードのとき、前記特権領域、前記 A P I 領域および前記ユーザ領域へのデータアクセスおよび命令アクセスを許可し、前記モード決定回路によって決定された動作モードが A P I モードのとき、前記 A P I 領域へのデータアクセスおよび命令アクセスと、前記ユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスおよび命令アクセスを禁止し

、前記モード決定回路によって決定された動作モードがユーザモードのとき、前記 A P I 領域への命令アクセスと、前記ユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスおよび命令アクセスと、前記 A P I 領域へのデータアクセスとを禁止する

ことを特徴とするプロセッサ。

【請求項 7】

外部とのデータのやりとりを行う外部 I / F と、

プログラムを格納する命令 R O M と、

データを格納するデータメモリと、

前記外部 I / F を経由して追加されたプログラムを格納する拡張メモリと、

前記命令 R O M および前記拡張メモリに格納されたプログラムを実行する C P U と、

前記 C P U が実行している命令のプログラムカウンタ値に基づいて実行領域を判定する実行領域判定回路と、

特権フラグと、

N 個 (N は 2 以上の整数) のユーザフラグと、

前記特権フラグの値を判定する特権フラグ判定回路と、

前記ユーザフラグの値を判定するユーザフラグ判定回路と、

前記実行領域判定回路による判定結果と前記特権フラグ判定回路による判定結果と前記ユーザフラグ判定回路による判定結果とに従って動作モードを決定するモード決定回路と、

前記モード決定回路によって決定された動作モードとアクセスアドレスとによって許可されないアクセスが発生した場合に割り込み要求を出力する不正アクセス検出回路とを備える

ことを特徴とするプロセッサ。

10

20

30

40

50

【請求項 8】

請求項 7 において、

前記モード決定回路によって決定される動作モードには、特権モード、A P I モード、ユーザモードが含まれ、

論理アドレス空間は、特権領域、A P I 領域、第 1 から第 N のユーザ領域に区分され、前記命令 R O M には前記特権領域および前記 A P I 領域、前記データメモリには前記特権領域、前記 A P I 領域および前記第 1 から第 N のユーザ領域、前記拡張メモリには前記第 1 から第 N のユーザ領域、前記特権フラグには A P I 領域、前記第 1 から第 N のユーザフラグには前記第 1 から第 N のユーザ領域が割り当てられ、

前記モード決定回路は動作モードを、前記特権領域または前記 A P I 領域上のプログラム実行時でありかつ前記特権フラグが O N のときには特権モード、前記 A P I 領域上のプログラム実行時でありかつ前記特権フラグが O F F のときは A P I モード、第 M ($1 \leq M \leq N$) のユーザ領域上のプログラム実行時でありかつ第 M のユーザフラグが O N のとき第 M のユーザモードとする

ことを特徴とするプロセッサ。

【請求項 9】

請求項 8 において、

不正アクセス検出回路は、

前記モード決定回路によって決定された動作モードが特権モードのとき、前記特権領域、前記 A P I 領域および前記第 1 から第 N のユーザ領域へのデータアクセスおよび命令アクセスを許可し、

前記モード決定回路によって決定された動作モードが A P I モードのとき、前記 A P I 領域へのデータアクセスおよび命令アクセスと、前記第 1 から第 N のユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスおよび命令アクセスを禁止し、

前記モード決定回路によって決定された動作モードが前記第 M のユーザモードのとき、前記 A P I 領域への命令アクセスと、前記第 M のユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスおよび命令アクセスと、前記 A P I 領域へのデータアクセスと、前記第 1 から第 N のユーザ領域のうち前記 M のユーザ領域以外の領域へのデータアクセスおよび命令アクセスとを禁止する

ことを特徴とするプロセッサ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明はプロセッサに関し、さらに詳しくは、メモリ保護機能を有するプロセッサに関する。

【0002】

【従来の技術および発明が解決しようとする課題】

近年、流通・サービス分野や交通分野などで I C カードが普及しつつある。I C カードには、ユーザプログラム（アプリケーションプログラム）をダウンロードして実行可能なものがある。このような I C カードには書き換え可能な不揮発性メモリ（たとえばフラッシュメモリ）が内蔵されており、この不揮発性メモリにユーザプログラムがダウンロードされる。上述の I C カードにはさらに命令 R O M（読み出し専用不揮発性メモリ）・データ R A M ・C P U が内蔵されている。命令 R O M には O S やサービスプログラムが格納される。命令 R O M および書き換え可能な不揮発性メモリに格納されたプログラムに従って C P U が各種の処理を行う。

【0003】

しかしながら上述の I C カードでは、書き換え可能な不揮発性メモリにダウンロードしたユーザプログラムによって命令 R O M 上のプログラムを不正に読み出したりデータ R A M 上のデータを不正に読み出し／書き込んだりすることが可能でありセキュリティが十分に

は確保されない。

【0004】

この発明の目的は、セキュリティを高めることができるプロセッサを提供することである。

【0005】

【特許文献1】

特開2000-76135号公報

【特許文献2】

特開2002-91826号公報

【特許文献3】

特開平11-238016号公報

【0006】

【課題を解決するための手段および発明の効果】

この発明によるプロセッサは、データ・演算処理を行うCPUと、プログラムを格納する命令ROMと、データを格納するデータRAMと、外部とのデータのやりとりを行う外部I/Fと、外部I/Fを経由してプログラムを格納する拡張メモリと、CPUから出力される実行している命令のプログラムカウンタ値にしたがって動作モードを決定するモード決定回路と、モード決定回路からの出力と命令ROM、データRAM、拡張メモリへのアクセスアドレス情報にしたがって不正なアクセスを検出する不正アクセス検出回路から構成され、メモリ領域を特権領域、API領域、ユーザ領域の3つに区分し、実行プログラムが配置されている領域にしたがってアクセス可能領域を設け、不正なアクセスが検出された場合は割り込みを発生させることを特徴とする。これにより、外部から追加されたプログラムからのセキュリティを確保することができる。

【0007】

【発明の実施の形態】

以下、この発明の実施の形態を図面を参照して詳しく説明する。なお、図中同一または相当部分には同一の符号を付しその説明は繰り返さない。

【0008】

(第1の実施形態)

<ICカードの全体構成>

第1の実施形態によるICカードの構成を図1に示す。このICカードは非接触型のICカードであり、アンテナコイル1とプロセッサ(ICチップ)2とを備える。プロセッサ2は、CPU201と、外部インタフェース(I/F)210と、命令ROM(読み出し専用不揮発性メモリ)211と、RAM212と、フラッシュメモリ(書き換え可能な不揮発性メモリ)213と、不正アクセス検出回路群220と、実行領域判定回路214と、モード決定回路215と、割り込みコントローラ216と、OR回路217とを備える。

【0009】

アンテナコイル1は、電磁結合によってリーダライタ(図示せず)から電力を受信しかつ情報の送受信を行う。外部I/F210は、プロセッサ2と外部(アンテナコイル1)との間のインタフェースである。

【0010】

命令ROM211には特権プログラム(OSやサービスプログラムなど)が格納される。フラッシュメモリ213にはユーザプログラム(アプリケーションプログラム)が格納される。フラッシュメモリ213に格納されるユーザプログラムはリーダライタ(図示せず)からアンテナコイル1および外部I/F210を介してダウンロードされる。

【0011】

CPU201は、命令ROM211およびフラッシュメモリ213に格納されているプログラムを実行する。CPU201は、実行している命令のプログラムカウンタ(PC)値S1を出力する。CPU201は、実行すべきメモリアクセスが命令アクセスであるかデ

10

20

30

40

50

ータアクセスであるかを示す信号 S 4 を出力する。ここでいう「命令アクセス」とは、実行すべき命令を読み込む（命令フェッチ）ためのメモリアクセスのことである。また「データアクセス」とは、読み込んだ命令の内容にメモリへのアクセスが含まれている場合におけるその命令の実行としてのメモリアクセスのことである。CPU 201 の内部には命令フェッチを制御する部分とデータアクセスを制御する部分とが存在する。命令フェッチを制御する部分からは命令フェッチ要求が発生し、データアクセスを制御する部分からはデータアクセス要求が発生する。CPU 201 は、これらの要求に応答してメモリアクセスを行う。命令フェッチ要求に応答してメモリアクセスを行うとき CPU 201 は、命令アクセスを示す信号 S 4 を出力する。データアクセス要求に応答してメモリアクセスを行うとき CPU 201 は、データアクセスを示す信号 S 4 を出力する。

10

【0012】

実行領域判定回路 214 は、CPU 201 によって実行されている命令が格納されている領域をプログラムカウンタ値 S 1 に基づいて判定する。領域の種類および区分については後に説明する。実行領域判定回路 214 は、判定された領域を示す信号 S 2 を出力する。

【0013】

モード決定回路 215 は、実行領域判定回路 214 からの信号 S 2 に基づいて動作モードを決定する。動作モードの種類については後に説明する。モード決定回路 215 は、決定した動作モードを示す信号 S 3 を出力する。

【0014】

不正アクセス検出回路群 220 は検出回路 221～223 を含む。検出回路 221 は、CPU 201 から命令 ROM 211 へのアクセスアドレスと信号 S 3～S 4 とに基づいて、CPU 201 から命令 ROM 211 へのアクセスを許可／禁止する。検出回路 222 は、CPU 201 から RAM 212 へのアクセスアドレスと信号 S 3～S 4 とに基づいて、CPU 201 から RAM 212 へのアクセスを許可／禁止する。検出回路 223 は、CPU 201 からフラッシュメモリ 213 へのアクセスアドレスと信号 S 3～S 4 とに基づいて、CPU 201 からフラッシュメモリ 213 へのアクセスを許可／禁止する。アクセスを許可するとき検出回路 221～223 は、CPU 201 からのアクセスアドレスを命令 ROM 211・RAM 212・フラッシュメモリ 213 へ与え、当該アドレスへのアクセス（書き込み／読み出し）を行う。アクセスを禁止するとき検出回路 221～223 は、CPU 201 からのアクセスアドレスを命令 ROM 211・RAM 212・フラッシュメモリ 213 へ与えず、検出信号 S 6 を出力する。

20

30

【0015】

OR 回路 217 は、割り込みコントローラ 216 からの割り込み信号 S 5 と検出回路 221～223 からの検出信号 S 6 との論理和を割り込み信号 S 7 として CPU 201 に与える。CPU 201 は、OR 回路 217 からの割り込み信号 S 7 に応答して割り込み処理を行う。

【0016】

<論理アドレス空間>

図 1 に示した IC カードの論理アドレス空間を図 2 に示す。論理アドレス空間は、特権領域と、API 領域と、ユーザ領域とに区分されている。アドレス a 3～a 4, a 7～a 8 が特権領域に割り当てられる。アドレス a 5～a 6, a 9～a 10 が API 領域に割り当てられる。アドレス a 1～a 2, a 11～a 12, a 13～a 14 がユーザ領域に割り当てられる。外部 I/F 210 にはアドレス a 1～a 2（ユーザ領域）が割り当てられる。命令 ROM 211 にはアドレス a 3～a 4（特権領域）、a 5～a 6（API 領域）が割り当てられる。RAM 212 にはアドレス a 7～a 8（特権領域）、a 9～a 10（API 領域）、a 11～a 12（ユーザ領域）が割り当てられる。フラッシュメモリ 213 にはアドレス a 13～a 14（ユーザ領域）が割り当てられる。

40

【0017】

<メモリ保護機能>

次に、図 1 に示した IC カードの動作について説明する。

50

【0018】

ICカードのROM 211には、OSやサービスプログラムなどの特権プログラムがあらかじめ格納されている。この特権プログラムはICカードの発行者によって保証されているプログラムである。ICカードのユーザは、所望のユーザプログラムをフラッシュメモリ 213にダウンロードする。フラッシュメモリ 213にダウンロードされたユーザプログラムは、ROM 211に格納されているOS上で動作する。

【0019】

CPU 201は、命令ROM 211およびフラッシュメモリ 213に格納されているプログラムを実行する。CPU 201はパイプライン処理を行う。パイプラインの段数は5段である。命令フェッチステージでは命令のフェッチ、デコードステージでは命令のデコード、実行ステージでは命令の実行、データアクセスステージではデータアクセス、ライトバックステージでは実行結果のレジスタへの書き込みがそれぞれ行われる。

10

【0020】

実行領域判定回路 214は、デコードステージで処理されている命令が格納されている領域（実行領域）を示す信号S2を出力する。デコードステージで処理されている命令に対応するプログラムカウンタ値S1がアドレスa3～a4に属するとき実行領域判定回路 214は、特権領域を示す信号S2を出力する（図2参照）。デコードステージで処理されている命令に対応するプログラムカウンタ値S1がアドレスa5～a6に属するとき実行領域判定回路 214は、API領域を示す信号S2を出力する（図2参照）。デコードステージで処理されている命令に対応するプログラムカウンタ値S1がアドレスa13～a14に属するとき実行領域判定回路 214は、ユーザ領域を示す信号S2を出力する（図2参照）。

20

【0021】

モード決定回路 215は、動作モードを示す信号S3を出力する。図3に示すように、実行領域判定回路 214からの信号S2が特権領域を示すときモード決定回路 215は、特権モードを示す信号S3を出力する。信号S2がAPI領域を示すときモード決定回路 215は、APIモードを示す信号S3を出力する。信号S2がユーザ領域を示すときモード決定回路 215は、ユーザモードを示す信号S3を出力する。このように、デコードステージで処理されている命令が格納されている領域（実行領域）に基づいて動作モードが決定される。

30

【0022】

検出回路 221～223は、モード決定回路 215からの信号S3が示す動作モードと、CPU 201からのアクセスアドレスが属する領域（アクセス領域）と、信号S4が示すアクセス種別（データアクセス、命令アクセス）とに基づいてメモリ 211～213へのアクセスを許可／禁止する。具体的には図4に示すように、動作モードが特権モードのとき検出回路 221～223はアクセス領域（特権領域、API領域、ユーザ領域）およびアクセス種別にかかわらずメモリ 211～213へのアクセスを許可する。動作モードがAPIモードのとき検出回路 221～223は、メモリ 211～213の特権領域へのデータアクセスを禁止し、それ以外のメモリアクセス（特権領域への命令アクセス、API領域へのデータアクセスおよび命令アクセス、ユーザ領域へのデータアクセスおよび命令アクセス）を許可する。動作モードがユーザモードのとき検出回路 221～223は、特権領域へのデータアクセスおよび命令アクセスとAPI領域へのデータアクセスとを禁止し、API領域への命令アクセスとユーザ領域へのデータアクセスおよび命令アクセスとを許可する。

40

【0023】

図5はメモリアクセス時のフローチャートである。

【0024】

ユーザモードのとき、メモリアクセスが特権領域へのアクセスの場合（ST11でYES）、不正アクセスとして割り込みが発生する（ST12）。したがって、ユーザ領域から特権領域へ直接に分岐することはできない。API領域へのアクセスの場合（ST13で

50

YES)、それがデータアクセスであれば不正アクセスとして割り込みが発生し(ST14~ST15)、命令アクセスであればAPI領域への命令アクセスを実行する(ST14, ST17)。ユーザ領域へのアクセスであれば(ST16)、アクセスを実行する(ST17)。

【0025】

APIモードのとき、メモリアクセスが特権領域へのアクセスの場合(ST21でYES)、それがデータアクセスであれば(ST22でYES)、不正アクセスとして割り込みが発生し(ST23)、命令アクセスであれば(ST22でNO)特権領域への命令アクセスを実行する(ST25)。API領域またはユーザ領域へのアクセスであれば(ST24)、アクセスを実行する(ST25)。

10

【0026】

特権モードのとき、どの領域に対しても制限なくアクセスを実行する(ST31)。

【0027】

図6は動作モード遷移時のパイプラインチャート図である。図6に示すように、ユーザ領域からAPI領域への分岐、API領域から特権領域への分岐の際に、それぞれユーザモードでのAPI領域へのメモリアクセス、APIモードでの特権領域へのメモリアクセスが発生するが、ともに命令アクセスであるのでアクセスは許可される。

【0028】

<効果>

以上のように第1の実施形態では、実行しているプログラムが格納されている領域とアクセス種別(命令アクセス/データアクセス)とに応じてメモリ211~213へのアクセスを制限している。具体的には、メモリ211~213の論理アドレス空間を特権領域とユーザ領域とAPI領域とに分割し、ユーザ領域から特権領域への分岐の際には必ずAPI領域を経由するようにしている。特権領域およびAPI領域のプログラムは命令ROM211に存在し、このプログラムはICカード発行者によって保証された(正しい)プログラムである。API領域を経由して特権領域に分岐することによって、特権領域中の決められた番地にのみ分岐することを保証している。これにより、ユーザ領域上のプログラムによる特権領域への不正アクセスを防ぐことができる。すなわち特権領域のプログラムおよびデータをユーザプログラムから保護することができる。

20

【0029】

(第2の実施形態)

<ICカードの全体構成>

第2の実施形態によるICカードの構成を図7に示す。このICカードは、図1に示したICカードの構成に加えてさらに検出回路224と、特権フラグ231と、特権フラグ判定回路232とを備える。

【0030】

特権フラグ判定回路232は、特権フラグ231の出力に従って特権フラグのON/OFFを判定し、判定結果(特権フラグ231がONであるかOFFであるか)を示す信号S8を出力する。

【0031】

モード決定回路215は、実行領域判定回路214からの信号S2と特権フラグ判定回路232からの信号S8とに基づいて動作モードを決定する。

40

【0032】

検出回路224は、CPU201から特権フラグ231へのアクセスアドレスと信号S3~S4とに基づいて、CPU201から特権フラグ231へのアクセスを許可/禁止する。アクセスを禁止するとき検出回路224は検出信号S6を出力する。

【0033】

<論理アドレス空間>

図7に示したICカードの論理アドレス空間を図8に示す。外部I/F210、命令ROM211、RAM212およびフラッシュメモリ213については第1の実施形態と同様

50

である（図2参照）。ここではさらにアドレスa15がAPI領域に割り当てられる。特権フラグ231にアドレスa15（API領域）が割り当てられる。

【0034】

<メモリ保護機能>

次に、図7に示したICカードの動作について説明する。ここでは第1の実施形態と異なる部分について説明する。

【0035】

モード決定回路215は、動作モードを示す信号S3を出力する。図9に示すように、実行領域判定回路214からの信号S2が特権領域を示しかつ特権フラグ判定回路232からの信号S8が特権フラグ231がONであることを示すときモード決定回路215は、特権モードを示す信号S3を出力する。信号S2がAPI領域を示しかつ信号S8が特権フラグ231がONであることを示すときモード決定回路215は、特権モードを示す信号S3を出力する。信号S2がAPI領域を示しかつ信号S8が特権フラグ231がOFFであることを示すときモード決定回路215は、APIモードを示す信号S3を出力する。信号S2がユーザ領域を示しかつ信号S8が特権フラグがOFFであることを示すときモード決定回路215は、ユーザモードを示す信号S3を出力する。このように、デコードステージで処理されている命令が格納されている領域（実行領域）と特権フラグ231のON/OFFとに基づいて動作モードが決定される。

【0036】

検出回路221～224は、モード決定回路215からの信号S3が示す動作モードと、CPU201からのアクセスアドレスが属する領域（アクセス領域）と、信号S4が示すアクセス種別（データアクセス、命令アクセス）とに基づいてメモリ211～213および特権フラグ231へのアクセスを許可/禁止する。具体的には図10に示すように、動作モードが特権モードのとき検出回路221～224はアクセス領域（特権領域、API領域、ユーザ領域）およびアクセス種別にかかわらずメモリ211～213および特権フラグ231へのアクセスを許可する。動作モードがAPIモードのとき検出回路221～224は、特権領域へのデータアクセスおよび命令アクセスを禁止し、API領域へのデータアクセスおよび命令アクセスとユーザ領域へのデータアクセスおよび命令アクセスとを許可する。動作モードがユーザモードのとき検出回路221～224は、特権領域へのデータアクセスおよび命令アクセスとAPI領域へのデータアクセスとを禁止し、API領域への命令アクセスとユーザ領域へのデータアクセスおよび命令アクセスとを許可する。

【0037】

図11は動作モード間の遷移を示す図である。

【0038】

特権モードからユーザモードに遷移する場合、まずAPI領域に分岐して、特権フラグ231をOFFにすることによってAPIモードに遷移する。このとき、特権領域上で特権フラグ231をOFFにするとAPIモードに遷移するが、特権領域への不正アクセスとなり割り込みが発生する。APIモードへの遷移後、ユーザ領域に分岐することによって、ユーザモードに遷移する。

【0039】

ユーザモードから特権モードに遷移する場合、まずAPI領域に分岐した後に、特権フラグ231をONにすることによって、特権モードに遷移する。

【0040】

図12はメモリアクセス時のフローチャートである。

【0041】

ユーザモードのとき、メモリアクセスが特権領域へのアクセスの場合（ST41でYES）、不正アクセスとして割り込みが発生する（ST42）。API領域へのアクセスの場合（ST43でYES）、データアクセスであれば（ST44でYES）、不正アクセスとして割り込みが発生し（ST45）、命令アクセスであれば（ST44でNO）API

領域への命令アクセスを実行する（S T 4 7）。ユーザ領域へのアクセスであれば（S T 4 6）、アクセスを実行する（S T 4 7）。

【0042】

A P Iモードのとき、メモリアクセスが特権領域へのアクセスの場合（S T 5 1でY E S）、不正アクセスとして割り込みが発生し（S T 5 2）、それ以外の領域へのアクセスであれば（S T 5 3）、アクセスを実行する（S T 5 4）。

【0043】

特権モードのとき、どの領域に対しても制限なくアクセスを実行する（S T 5 5）。

【0044】

図13はモード遷移時のパイプラインチャート図である。ユーザ領域からA P I領域への分岐の際に、ユーザモードでのA P I領域へのメモリアクセスが発生するが命令アクセスであるのでアクセスは許可される。また、A P Iモードでの特権フラグのセットによって特権モードに遷移する。

【0045】

<効果>

第2の実施形態によれば第1の実施形態におけるのと同様の効果が得られる。さらに、ユーザ領域から特権領域への分岐の際には「A P I領域での特権フラグへのデータアクセス」が必要となるため、特権モードに遷移する前に必ずユーザ領域でのメモリアクセスが完了することになる。

【0046】

（第3の実施形態）

<I Cカードの全体構成>

第3の実施形態によるI Cカードの構成を図14に示す。このI Cカードは、図7に示したI Cカードの構成に加えてさらに検出回路225と、ユーザフラグ240と、ユーザフラグ判定回路251とを備える。

【0047】

ユーザフラグ240はN個のフラグ（ユーザフラグ1～ユーザフラグN）を含む。

【0048】

ユーザフラグ判定回路251は、ユーザフラグ240の出力に従ってユーザフラグ1～ユーザフラグNのO N / O F Fを判定し、判定結果（ユーザフラグ1～ユーザフラグNがO NであるかO F Fであるか）を示す信号S9を出力する。

【0049】

モード決定回路215は、実行領域判定回路214からの信号S2と特権フラグ判定回路232からの信号S8とユーザフラグ判定回路251からの信号S9とに基づいて動作モードを決定する。

【0050】

検出回路225は、C P U 201からユーザフラグ240（ユーザフラグ1～N）へのアクセスアドレスと信号S3～S4とに基づいて、C P U 201からユーザフラグ240（ユーザフラグ1～N）へのアクセスを許可／禁止する。アクセスを禁止するとき検出回路225は検出信号S6を出力する。

【0051】

<論理アドレス空間>

図14に示したI Cカードの論理アドレス空間を図15に示す。ここではR A M 212およびフラッシュメモリ213のユーザ領域がN個の領域（ユーザ領域1～ユーザ領域N）に分割される。さらにアドレスa16～a16+Nがユーザ領域1～Nに割り当てられる。ユーザフラグ1～Nにアドレスa16（ユーザ領域1）～a16+N（ユーザ領域N）が割り当てられる。

【0052】

<メモリ保護機能>

次に、図14に示したI Cカードの動作について説明する。ここでは第1および第2の実

10

20

30

40

50

施形態と異なる部分について説明する。

【0053】

モード決定回路215は、動作モードを示す信号S3を出力する。図16に示すように、実行領域判定回路214からの信号S2が特権領域またはAPI領域を示しかつ特権フラグ判定回路232からの信号S8が特権フラグ231がONであることを示すときモード決定回路215は、特権モードを示す信号S3を出力する。なお、ユーザフラグ1～NはONであってもOFFであってもかまわない。信号S2がAPI領域を示しかつ信号S8が特権フラグ231がOFFであることを示すときモード決定回路215は、APIモードを示す信号S3を出力する。なお、ユーザフラグ1～NはONであってもOFFであってもかまわない。信号S2がユーザ領域1を示しかつ信号S8が特権フラグ231がOFFであることを示しかつ信号S9がユーザフラグ1がONでありユーザフラグ2～NがOFFであることを示すときモード決定回路215は、ユーザモード1を示す信号S3を出力する。同様に、信号S2がユーザ領域M ($2 \leq M \leq N$) を示しかつ信号S8が特権フラグ231がOFFであることを示しかつ信号S9がユーザフラグMがONでありユーザフラグ1～N (ただしMを除く) がOFFであることを示すときモード決定回路215は、ユーザモードMを示す信号S3を出力する。このように、デコードステージで処理されている命令が格納されている領域(実行領域)と特権フラグ231のON/OFFとユーザフラグ1～NのON/OFFとに基づいて動作モードが決定される。

【0054】

検出回路221～225は、モード決定回路215からの信号S3が示す動作モードと、CPU201からのアクセスアドレスが属する領域(アクセス領域)と、信号S4が示すアクセス種別(データアクセス、命令アクセス)とに基づいてメモリ211～213、特権フラグ231およびユーザフラグ1～Nへのアクセスを許可/禁止する。具体的には図17に示すように、動作モードが特権モードのとき検出回路221～225はアクセス領域(特権領域、API領域、ユーザ領域、ユーザ領域1～N)およびアクセス種別にかかわらずメモリ211～213、特権フラグ231およびユーザフラグ1～Nへのアクセスを許可する。動作モードがAPIモードのとき検出回路221～225は、特権領域へのデータアクセスおよび命令アクセスを禁止し、それ以外の領域(API領域、ユーザ領域、ユーザ領域1～N)へのデータアクセスおよび命令アクセスを許可する。動作モードがユーザモードM ($1 \leq M \leq N$) のとき検出回路221～225は、API領域への命令アクセスと、ユーザ領域へのデータアクセスおよび命令アクセスと、ユーザ領域Mへのデータアクセスおよび命令アクセスとを許可し、特権領域へのデータアクセスおよび命令アクセスと、API領域へのデータアクセスと、ユーザ領域1～N (ただしMを除く) へのデータアクセスおよび命令アクセスとを禁止する。

【0055】

図18はモード遷移を表す図である。特権モードのとき、特権領域もしくはAPI領域上のプログラムを実行中である。特権モードからAPIモードに遷移する場合、まずAPI領域に分岐し、特権フラグ231をOFFにする。APIモードからユーザモードNに遷移する場合、API領域において、ユーザフラグNをONにした後にユーザ領域Nに分岐する。ユーザフラグNがOFFの状態ではユーザ領域Nに分岐した場合、不正アクセスと判定されて割り込みが発生する。次に、あるユーザ領域から別のユーザ領域に遷移する場合を説明する。ユーザ領域Nからユーザ領域M ($0 < M < N$) に遷移する場合、ユーザフラグMをONにするためにAPI領域に分岐(APIモードに遷移)する。その後で、ユーザフラグNをOFF、ユーザフラグMをONにし、ユーザ領域Mに分岐する。

【0056】

<効果>

以上のように第3の実施形態によれば、ユーザプログラムから特権領域やほかのユーザ領域への不正なアクセスを防止することができる。

【図面の簡単な説明】

【図1】第1の実施形態によるICカードの全体構成を示すブロック図である。

10

20

30

40

50

- 【図 2】 図 1 に示した IC カードの論理アドレス空間を示す図である。
 【図 3】 実行領域と動作モードとの対応関係を示す図である。
 【図 4】 各動作モードにおいてアクセスを許可／禁止する領域を示す図である。
 【図 5】 メモリアクセス時のフローチャートである。
 【図 6】 モード遷移時のパイプラインチャート図である。
 【図 7】 第 2 の実施形態による IC カードの全体構成を示すブロック図である。
 【図 8】 図 7 に示した IC カードの論理アドレス空間を示す図である。
 【図 9】 実行領域および特権フラグと動作モードとの対応関係を示す図である。
 【図 10】 各動作モードにおいてアクセスを許可／禁止する領域を示す図である。
 【図 11】 動作モード間の遷移を示す図である。
 【図 12】 メモリアクセス時のフローチャートである。
 【図 13】 モード遷移時のパイプラインチャート図である。
 【図 14】 第 3 の実施形態による IC カードの全体構成を示すブロック図である。
 【図 15】 図 14 に示した IC カードの論理アドレス空間を示す図である。
 【図 16】 実行領域、特権フラグおよびユーザフラグと動作モードとの対応関係を示す図である。

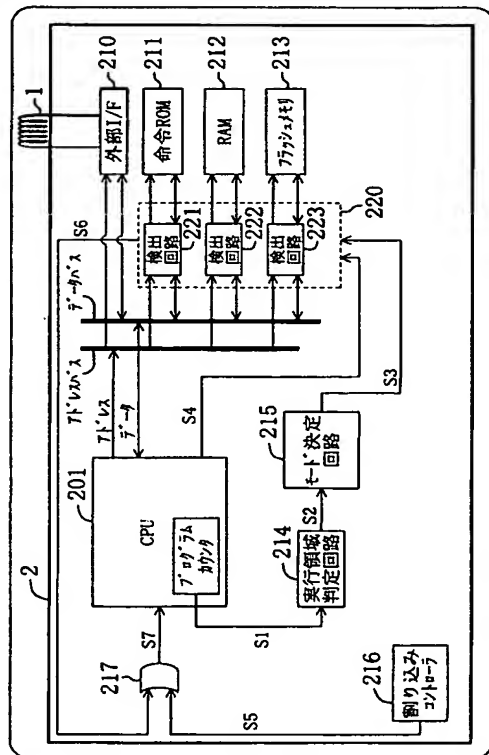
【図 17】 各動作モードにおいてアクセスを許可／禁止する領域を示す図である。

【図 18】 動作モード間の遷移を示す図である。

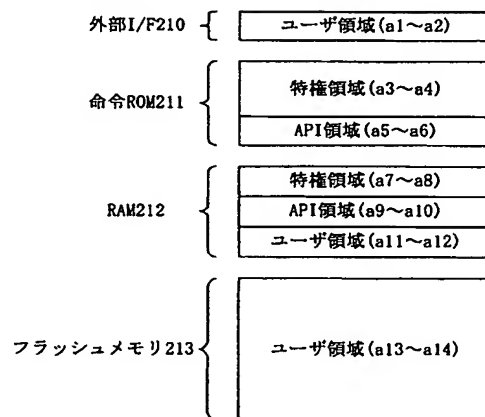
【符号の説明】

201 CPU、210 外部 I/F、211 命令 ROM、212 RAM（データメモリ）、213 フラッシュメモリ（拡張メモリ）、214 実行領域判定回路、215 モード決定回路、220 不正アクセス検出回路群。

【図 1】



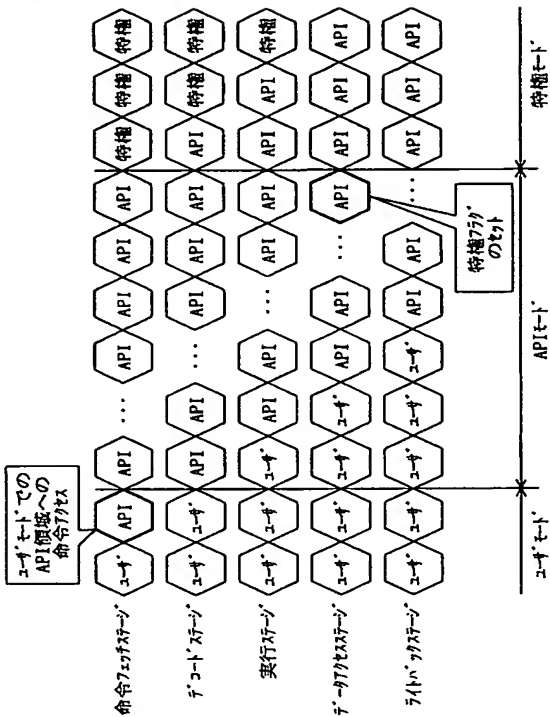
【図 2】



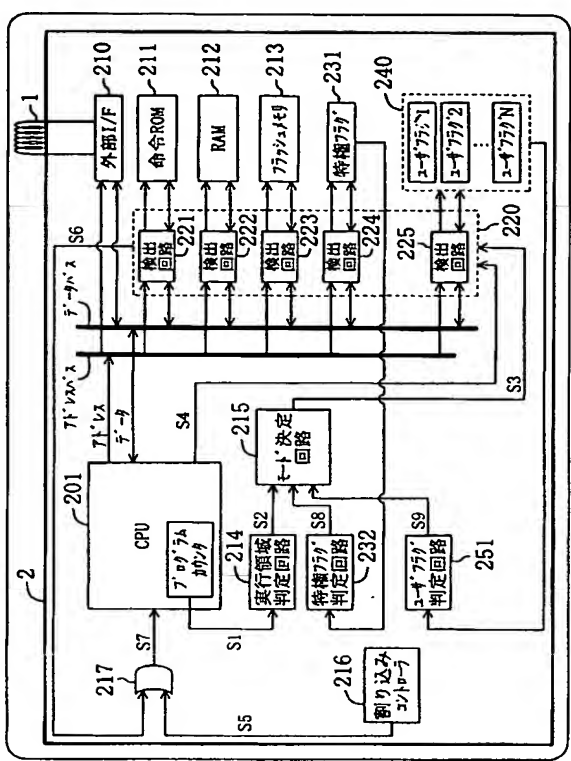
【図 3】

実行領域 (S2)	動作モード (S3)
特権領域	特権モード
API領域	APIモード
ユーザ領域	ユーザモード

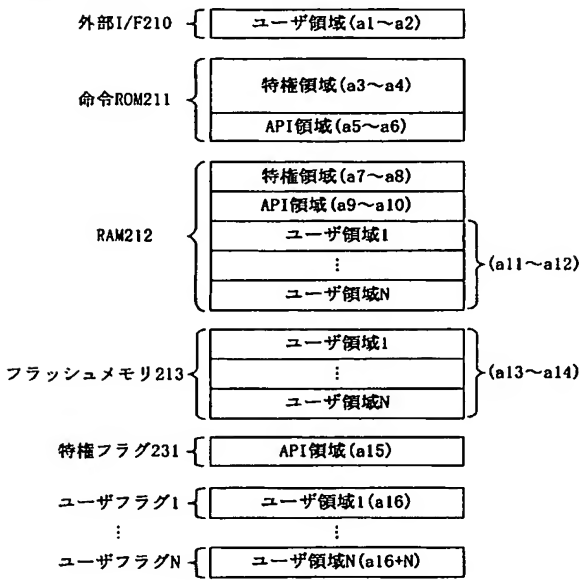
【図 13】



【図 14】



【図 15】



【図 16】

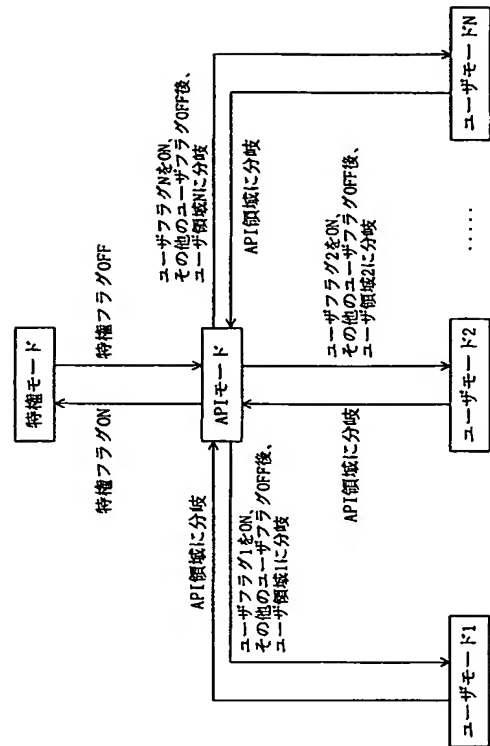
実行領域(S2)	特権フラグ(S6)	ユーザフラグ1	ユーザフラグ2	...	ユーザフラグN	動作モード(S3)
特権領域/API領域	ON	ON/OFF	ON/OFF	...	ON/OFF	特権モード
API領域	OFF	ON/OFF	ON/OFF	...	ON/OFF	APIモード
ユーザ領域1	OFF	ON	OFF	...	OFF	ユーザモード1
ユーザ領域2	OFF	OFF	ON	...	ON	ユーザモード2
...
ユーザ領域N	OFF	OFF	OFF	...	ON	ユーザモードN

【図 17】

API領域 および API種別	特権領域		API領域		ユーザ領域		ユーザ領域1		ユーザ領域2		ユーザ領域N	
	データ アクセス	命令 アクセス	データ アクセス	命令 アクセス	データ アクセス	命令 アクセス	データ アクセス	命令 アクセス	データ アクセス	命令 アクセス	データ アクセス	命令 アクセス
動作モード												
特権モード	○	○	○	○	○	○	○	○	○	○	○	○
APIモード	×	×	○	○	○	○	○	○	○	○	○	○
ユーザモード1	×	×	×	○	○	○	○	×	×	×	×	×
ユーザモード2	×	×	×	○	○	○	×	○	○	×	×	×
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
ユーザモードN	×	×	×	○	○	○	×	×	×	×	○	○

○……許可, X……禁止

【図 18】



フロントページの続き

(74)代理人 100115510

弁理士 手島 勝

(74)代理人 100115691

弁理士 藤田 篤史

(72)発明者 長谷部 朋哉

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

F ターム(参考) 5B017 AA01 BA01 BA06 CA11 CA14

5B035 BB09 CA11 CA23 CA38

5B076 FB02